METHOD AND APPARATUS FOR PROTECTION OF CONTENT USING BIOMETRIC WATERMARKS

The present invention relates to methods and systems for the protection of digital content through the use of watermark techniques, and more particularly, for encoding, detecting and verifying watermarks that include biometric information.

Watermarks are embedded signatures in content (e.g., video and audio content) to verify the source of the material. This enables the owners and distributors of content to control and protect their copyrights and other ownership interests, and to control the distribution of the content. The goal of a digital watermark system is to embed an information signal or signals in the content such that there are few or no artifacts in the underlying content signal, while maximizing the encoding level and location sensitivity such that any attempt to remove the watermark will cause damage to the content signal. Generally, a digital watermark is difficult to remove because it shares many of the characteristics of random or pseudo-random noise within the digital content.

Watermarked digital content is typically embedded with a payload of information within the watermark, such as the names of the content author and content distributor. When the watermarked content is accessed by a device that has a watermark detection capability, such as a DVD player, a search for the watermark and evaluation of the watermark payload information is typically performed utilizing a watermark detection technique that is associated with that type of watermark. If the proper watermark is found, the device will permit play-out of the content. If the watermark is not detected or a corrupted watermark is detected, however, the device will not permit access to the watermarked content. Thus, the illegal reproduction and distribution of content will be prohibited.

The widespread use of the Internet has provided an additional outlet for the purchasing and downloading of multimedia content. However, peer-to-peer file sharing causes additional problems, such as content piracy. Digital watermarking and encryption techniques have been used to protect content and reduce piracy attributed to peer-to-peer file sharing. For example, if a first user legally obtains an encrypted file, the user has the key for decoding the content. To prevent the first user plans from sharing the content and associated key with a second user, the content is typically encoded with